Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premise integrations

Sunday Adeola Oladosu [1,*], Christian Chukwuemeka Ike [2], Peter Adeyemo Adepoju [3], Adeoye Idowu Afolabi [4], Adebimpe Bolatito Ige [5] and Olukunle Oladipupo Amoo [6]

[1] *Independent Researcher, Texas, USA.*
[2] *Globacom Nigeria Limited.*
[3] *Independent Researcher, Lagos, Nigeria.*
[4] *CISCO, Nigeria.*
[5] *Independent Researcher, Canada.*
[6] *Amstek Nigeria Limited.*

Magna Scientia Advanced Research and Reviews, 2021, 03(01), 079–090

Publication history: Received on 10 September 2021; revised on 18 October 2021; accepted on 21 October 2021

Article DOI: https://doi.org/10.30574/msarr.2021.3.1.0076

Abstract

As organizations increasingly adopt hybrid cloud environments, the complexity of managing and securing these infrastructures has grown. Hybrid cloud and on-premise integrations present unique challenges in terms of data security, access control, and compliance, requiring a more advanced and unified approach to cloud networking security. This review conceptualizes a unified security framework aimed at addressing the specific security needs of hybrid cloud and on-premise integrations. The framework is designed to balance the flexibility and scalability of cloud environments with the robustness of on-premise systems, ensuring comprehensive protection across both landscapes. The proposed framework integrates key security principles, including the CIA triad (Confidentiality, Integrity, and Availability), Zero trust security models, and advanced data encryption techniques to ensure secure data flows and interactions between hybrid environments. It emphasizes the use of automation and orchestration to streamline security policy enforcement, incident detection, and response, ensuring that security operations are efficient and consistent across diverse infrastructures. Additionally, the framework focuses on compliance and regulatory requirements, ensuring continuous monitoring, auditing, and reporting to maintain industry standards such as GDPR, HIPAA, and CCPA. The review also examines various security technologies crucial for hybrid cloud environments, including cloud-native security tools, VPNs, SD-WAN, and multi-factor authentication (MFA). Case studies from industries such as financial services and manufacturing illustrate how the proposed security model can be successfully applied, offering tangible benefits in terms of enhanced security and operational efficiency. By conceptualizing a unified security framework for hybrid cloud and on-premise integrations, this review provides organizations with a roadmap to mitigate security risks, optimize network operations, and achieve compliance. It concludes with insights into future trends in cloud security, including the role of artificial intelligence and quantum computing in shaping the future of hybrid cloud security models.

Keywords: Cloud networking security models; Hybrid cloud; On-Premise integrations; Review

1. Introduction

Cloud networking security has become an essential aspect of modern IT infrastructures as organizations increasingly adopt cloud computing to streamline operations, enhance scalability, and reduce operational costs (Muhammad et al., 2018; Sehgal et al., 2020). Cloud environments provide flexibility and efficiency, enabling businesses to store data, run applications, and access computing resources on-demand. However, as organizations transition to cloud-based systems,

* Corresponding author: Sunday Adeola Oladosu.

they face the daunting task of ensuring robust security across a growing number of diverse platforms (Tabrizchi and Kuchaki, 2020). This challenge becomes particularly pronounced with the rise of hybrid cloud and on-premise infrastructures, which combine both public and private cloud systems with traditional on-premise networks.

Hybrid cloud environments integrate public cloud services with private cloud infrastructure and on-premise data centers, enabling organizations to scale their operations dynamically (Gundu et al., 2020). While hybrid cloud systems offer significant advantages such as cost optimization, flexibility, and workload management, they introduce significant complexity from a security standpoint. On-premise data centers and private clouds have traditionally relied on well-established security models, while public cloud services require different security strategies (Mthunzi et al., 2020). The interplay between these environments requires careful management of security protocols, tools, and policies to ensure seamless integration and protection across all platforms.

Securing hybrid environments is a multifaceted challenge because each environment has its own set of security requirements and protocols (Obaidat et al., 2020). On-premise infrastructures often focus on perimeter defense, access controls, and physical security, whereas cloud environments require a more flexible, scalable approach that accounts for dynamic resource allocation and varying levels of service provider responsibility. Organizations must navigate these differences while ensuring the integrity, confidentiality, and availability of their data and applications. Furthermore, the complexity of managing multiple security frameworks for disparate environments can lead to gaps in security, making it difficult to maintain consistent protection and increasing the risk of breaches or attacks (Kure et al., 2018; Anisetti et al., 2020).

The primary objective of this review is to explore the need for advanced cloud networking security models that can address the unique challenges posed by hybrid and multi-cloud environments. Traditional security models, which focus primarily on perimeter defense and internal network security, are inadequate for the complex, distributed nature of modern cloud networks. As organizations embrace hybrid cloud and on-premise systems, they require more integrated, adaptive, and intelligent security approaches that can offer real-time visibility, policy enforcement, and incident response across both cloud-based and on-premise environments (Raj et al., 2018; Gade, 2020).

A key focus of this exploration is the development of a unified security framework for hybrid cloud and on-premise integration. This framework will provide a holistic approach to securing these environments, accounting for the differences in architecture, access controls, and risk profiles of each platform. A unified security framework will not only streamline security operations by consolidating management tools and policies but also ensure that security protocols are consistent across all systems (Muhammad, 2019). It will integrate cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and automation to enhance threat detection, response times, and risk management. This will also include advanced encryption and authentication techniques tailored to the demands of hybrid cloud environments.

By conceptualizing this unified security model, the review aims to provide organizations with a practical solution that balances flexibility with security, enabling them to capitalize on the benefits of hybrid and multi-cloud infrastructures without compromising on data protection. The framework will seek to address the complexities of securing dynamic, scalable cloud networks while ensuring compliance with industry standards and regulations. Ultimately, the goal is to create a security architecture that can evolve alongside the ever-changing technological landscape, supporting seamless integration and robust protection for both cloud-native and on-premise systems.

2. Fundamentals of Cloud Networking and Security

Cloud networking refers to the use of virtualized networks that connect cloud-based resources, such as applications, storage, and computing services, over the internet or private connections (Spirin et al., 2019). These networks allow organizations to access resources on-demand, scale dynamically, and manage traffic without the need for traditional physical network infrastructure. Understanding cloud networking models is essential to comprehending the security challenges they present. The three primary types of cloud networking models are public, private, and hybrid clouds, each with its own set of benefits and limitations. Public Cloud is a model where cloud services are provided over the internet by third-party providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) (Kamal et al., 2020). In this model, infrastructure and services are shared with other organizations, which can reduce operational costs and increase scalability. However, organizations relying on public cloud solutions may face concerns about control, data privacy, and security risks from shared environments. Private Cloud refers to a cloud infrastructure that is owned and operated by a single organization, either on-premise or hosted by a third-party provider. This model offers greater control over data and security, as it is not shared with other organizations. While private clouds offer more tailored security measures, they come with higher costs, limited scalability, and increased management

complexity (Sunyaev, 2020). Hybrid Cloud combines elements of both public and private cloud systems. In a hybrid environment, an organization utilizes both on-premise infrastructure and public cloud resources to optimize performance, cost, and security. A key advantage of hybrid cloud is the flexibility it offers organizations to move workloads between public and private clouds based on factors like workload requirements, cost considerations, or regulatory compliance. However, hybrid clouds introduce significant complexity, particularly in terms of integrating and managing security across diverse environments. On-premise environments, while not a cloud model, still play a crucial role in modern IT architectures. On-premise systems typically consist of physical servers, storage, and networking equipment housed within an organization's own facilities. Although on-premise infrastructure gives organizations full control over their systems and security, it also requires significant investment in hardware, maintenance, and skilled personnel. In hybrid cloud environments, the integration of on-premise systems with cloud services creates additional challenges for network management and security (Chiranjeevi et al., 2018). The need to coordinate data flow, optimize performance, and ensure consistent security policies across both private and public environments requires careful planning and execution.

Hybrid cloud environments, due to their inherent complexity, introduce several security challenges that organizations must address to ensure data protection and compliance (Trakadas et al., 2019). As organizations adopt hybrid cloud solutions, they must navigate risks associated with data migration, multi-cloud environments, and the involvement of third-party services. One of the primary challenges in hybrid cloud environments is the migration of data between on-premise infrastructure and public cloud services. Moving sensitive data to the cloud exposes it to potential breaches during transit. Data can be vulnerable if not properly encrypted or if adequate security controls are not in place during migration. Additionally, organizations must ensure that the cloud service provider complies with relevant data protection regulations, such as the General Data Protection Regulation (GDPR), to avoid the risk of non-compliance (Duncan and Zhao, 2018). The use of multiple cloud providers to meet different business needs, known as multi-cloud, has become a common practice. While multi-cloud strategies can provide increased redundancy, flexibility, and the ability to avoid vendor lock-in, they also introduce significant security complexities. These environments require organizations to manage disparate security policies, compliance standards, and access controls across different platforms, increasing the risk of security misconfigurations and gaps in visibility. Managing diverse cloud environments increases the likelihood of inconsistent security practices and complex threat landscapes (Sharma, 2020). Hybrid cloud architectures often rely on third-party services for additional functionalities, such as content delivery networks (CDNs), security tools, or SaaS applications. These services introduce external risk factors, as organizations may have limited visibility and control over their security protocols. When integrating these third-party services, organizations must ensure that security standards align with internal policies and that third-party vendors adhere to industry best practices. Furthermore, vulnerabilities in third-party services can become entry points for cyberattacks. The complexity of securing hybrid cloud environments arises primarily from the need to manage and enforce security across diverse platforms. Security challenges include: Ensuring proper access control policies are enforced across both cloud and on-premise systems is critical. Traditional network security practices often rely on perimeter defenses and role-based access control (RBAC), but these methods may not be effective in hybrid environments (Indu et al., 2018). Identity and access management (IAM) systems, which allow for fine-grained control over user and service permissions, are essential for ensuring that only authorized users and services can access sensitive resources. In hybrid environments, IAM must be integrated seamlessly across public and private cloud platforms to provide consistent access control. Protecting data both in transit and at rest is a critical security requirement for hybrid cloud environments. Organizations must implement encryption protocols that safeguard sensitive data as it moves between on-premise systems and the cloud, ensuring that unauthorized parties cannot intercept or tamper with it (Okechukwu et al., 2018; Pookandy, 2020). Additionally, data encryption must be consistent across both private and public cloud systems to avoid vulnerabilities during data transfers. Public cloud providers typically offer encryption tools, but organizations must ensure these tools meet their specific security requirements. Maintaining compliance with industry-specific regulations, such as HIPAA for healthcare or PCI-DSS for payment processing, becomes more complex in hybrid cloud environments. Organizations must ensure that their security practices, data storage, and access controls align with these regulations across all platforms. This requires continuous monitoring, auditing, and reporting mechanisms to maintain compliance, which can be challenging given the dynamic and distributed nature of hybrid cloud environments. Securing hybrid cloud environments requires an integrated approach that spans multiple cloud platforms and on-premise systems. Organizations must manage the complexity of diverse security requirements, access controls, and encryption methods to protect sensitive data and meet compliance standards (Hale and Gamble, 2019). Addressing these challenges effectively will enable businesses to harness the benefits of hybrid cloud solutions while minimizing risks to their security posture.

2.1. Key Principles for Cloud Security Models

Cloud security involves safeguarding the integrity, availability, and confidentiality of data and resources in cloud computing environments (Tchernykh et al., 2019). As businesses increasingly adopt hybrid cloud infrastructures, which integrate on-premise and public cloud services, a solid security framework is necessary to address the complexities of managing data protection across diverse systems. Several key principles underpin effective cloud security models, including the Confidentiality, Integrity, and Availability (CIA) Triad, Zero Trust Security Model, and Data Encryption and Secure Communication.

Confidentiality ensures that data is only accessible to authorized users and entities. In a hybrid cloud environment, where data is often shared across multiple platforms, maintaining confidentiality becomes more complex. Organizations must implement robust access control systems to restrict data access. Identity and access management (IAM) solutions are critical for enforcing strong authentication and authorization policies across both on-premise systems and cloud platforms (Anand and Khemchandani, 2019; El Sibai et al., 2020). Additionally, enforcing role-based access control (RBAC) ensures that users only have access to the data necessary for their tasks, reducing the risk of unauthorized data exposure. Integrity refers to the accuracy and consistency of data across cloud platforms. Ensuring data integrity requires mechanisms that verify the data's accuracy during transit and storage. Hybrid cloud architectures must use methods like checksum algorithms and digital signatures to detect and prevent data tampering during migration or while stored in the cloud. It is also vital to monitor data modifications and access patterns to identify any suspicious activity that could compromise data integrity. Availability ensures that data and services are accessible to authorized users when required. In hybrid environments, guaranteeing availability often requires managing the performance of systems across multiple clouds and on-premise infrastructures. Organizations must utilize redundancy, load balancing, and failover mechanisms to ensure high availability and prevent downtime, which is critical for ensuring business continuity (Abualkishik et al., 2020).

The Zero Trust Security Model is based on the principle that no one, whether inside or outside the network, should be trusted by default. In a hybrid cloud environment, this model becomes essential for continuously verifying the identity and trustworthiness of users, devices, and systems before granting access to resources (Zhou et al., 2018). Rather than relying on traditional perimeter-based security, Zero Trust demands that each user, device, and request be authenticated and authorized, regardless of their origin. Continuous Verification is a core principle of Zero Trust, where all access requests are treated as untrusted until verified. This means that even users within the organization's internal network must be authenticated each time they attempt to access sensitive data or applications. Implementing multi-factor authentication (MFA) and context-based authentication based on user behavior and access patterns ensures that only legitimate users gain access. Network Segmentation is another key aspect of Zero Trust. By segmenting networks into smaller, isolated zones, organizations can reduce the surface area for potential attacks. Each segment has its own security controls and policies, preventing lateral movement within the network in case of a breach. In hybrid cloud environments, this means segmenting cloud resources, on-premise systems, and even specific workloads to ensure that access to critical resources is tightly controlled (Hiran et al., 2019). Least-Privilege Access is a crucial Zero Trust principle, ensuring that users, applications, and services have the minimum necessary permissions to perform their tasks. By limiting the scope of access, organizations reduce the potential damage caused by compromised accounts or systems. This principle is especially vital in hybrid environments, where the attack surface is expanded across multiple platforms and cloud services.

Data encryption plays a pivotal role in ensuring the confidentiality and integrity of data in cloud environments (Megouache et al., 2020). Whether data is stored in cloud services or transmitted between different cloud platforms, it must be encrypted to prevent unauthorized access. In hybrid cloud systems, data is constantly moving between on-premise and cloud infrastructure, increasing the need for robust encryption strategies. End-to-End encryption is the process of encrypting data at its source and decrypting it only at the intended destination, ensuring that the data remains secure throughout its lifecycle. Implementing end-to-end encryption ensures that even if data is intercepted during transit, it cannot be read or modified by unauthorized parties. For hybrid cloud architectures, this involves encrypting data both in transit (e.g., through the use of SSL/TLS protocols for communication) and at rest (e.g., using Advanced Encryption Standard (AES) encryption for cloud storage). Securing data-in-transit involves encrypting communications between different cloud environments, ensuring that data remains confidential and intact while moving across public networks (Tan et al., 2018). Virtual Private Networks (VPNs), secure tunneling protocols, and encrypted APIs are commonly used to secure these connections. Additionally, Transport layer security is widely used to secure web-based communications, ensuring that data sent between clients and cloud services is protected from interception or modification. Securing data-at-rest is equally critical, as it protects stored data on cloud platforms or on-premise servers. Many cloud providers offer encryption options for data-at-rest, which organizations must enable to protect sensitive data. Additionally, organizations should implement key management systems (KMS) to control access

to encryption keys and ensure that keys are rotated regularly to maintain security. In hybrid cloud environments, securing communication and data across multiple platforms requires integration of encryption tools and security protocols across both on-premise and cloud systems. This integration ensures that encryption is consistent and that the security of data is maintained at every point in its lifecycle, whether it is stored locally or in a remote cloud environment. A robust cloud security model is essential for safeguarding data and services in hybrid cloud environments. By adhering to the principles of Confidentiality, Integrity, and Availability (CIA Triad), organizations can protect data from unauthorized access and tampering. The Zero Trust Security model ensures continuous verification and least-privilege access across diverse systems (Yan and Wang, 2020). Finally, data encryption and secure communication protocols safeguard data both at rest and in transit, ensuring that sensitive information remains protected across hybrid infrastructures. These foundational principles help organizations build a security architecture that can withstand evolving threats in today's complex hybrid cloud environments.

2.2. Designing a Unified Security Framework for Hybrid Cloud and On-Premise Integrations

As businesses increasingly adopt hybrid cloud architectures integrating on-premise data centers with public and private cloud environments the need for a unified security framework that spans these diverse infrastructures has never been more critical. A unified framework ensures that organizations can manage security risks, protect sensitive data, and maintain compliance across both cloud and on-premise systems (Plá et al., 2020). This section explores the key components necessary for designing such a framework, focusing on secure access control, integration of security monitoring, security automation, and compliance considerations. A robust security framework begins with ensuring secure access control and identity management across hybrid environments. The integration of Single Sign-On (SSO) and Identity and Access Management (IAM) systems is essential for enabling centralized authentication and authorization processes. IAM allows organizations to define, enforce, and manage access policies, ensuring that users and applications are granted appropriate access to resources based on roles, trust levels, and specific needs. This approach helps prevent unauthorized access to critical data, mitigating security risks from both internal and external threats. SSO further streamlines the user experience by enabling employees to access multiple systems with a single set of credentials, reducing the likelihood of credential fatigue and associated security vulnerabilities (Ranise et al., 2019). In addition to access control, security monitoring and incident detection across hybrid systems must be integrated. A comprehensive monitoring system provides visibility into both on-premise and cloud environments, enabling the continuous tracking of potential security incidents. Integration of security information and event management (SIEM) systems across hybrid infrastructures allows for real-time data collection and analysis from disparate security tools, providing a holistic view of the organization's security posture. These systems can detect unusual activity, potential threats, or breaches, triggering automated alerts and initiating response protocols. The integration of intrusion detection systems (IDS) and intrusion prevention systems (IPS) further enhances this capability, helping identify and mitigate threats at both the network and application levels (Cai et al., 2019).

Security automation and orchestration are critical for improving response times and reducing the manual effort required for security management. Automating the enforcement of security policies ensures that best practices are consistently applied across all systems, minimizing the risk of human error and ensuring compliance with organizational and regulatory standards (Mughal , 2019; Shneiderman, 2020). Automated processes can manage tasks such as vulnerability scanning, patch management, access controls, and incident response, allowing security teams to focus on more complex issues. Automated tools can quickly detect threats and initiate pre-defined responses, such as isolating compromised systems, alerting the security team, and mitigating further damage. Security orchestration involves integrating a variety of security tools into a unified system to ensure streamlined communication and coordination. By using orchestration platforms, organizations can manage their security stack from a centralized interface, improving visibility and reducing the complexity of managing multiple tools across hybrid environments. This centralized approach enhances the efficiency of security operations by enabling automated workflows that span across both cloud and on-premise infrastructures. Orchestration also allows organizations to automate the deployment of security updates, thus reducing the window of vulnerability and ensuring consistent protection across all systems (Kumar and Goyal, 2020).

As organizations face growing pressure to comply with industry-specific regulations, a unified security framework must be designed with compliance in mind. Regulations such as GDPR, HIPAA, and CCPA dictate strict requirements regarding data protection, privacy, and reporting, making it essential for the security framework to include compliance mechanisms (Hartzog and Richards, 2020). The framework must ensure that sensitive data is protected according to these regulations, with controls in place to prevent unauthorized access or breaches. To maintain continuous compliance, organizations must implement robust auditing and reporting mechanisms. These systems provide ongoing oversight of security policies and practices, ensuring that organizations can demonstrate adherence to regulatory requirements. Automated auditing tools can track activities across both cloud and on-premise systems, generating real-

time reports that highlight areas of non-compliance and suggesting corrective actions. Additionally, data residency and data protection rules must be taken into account when designing the framework, particularly in hybrid cloud systems that span multiple jurisdictions with varying compliance requirements. Continuous compliance monitoring ensures that security practices evolve to meet the latest regulatory standards, reducing the risk of non-compliance fines or reputational damage. Security frameworks that incorporate automated auditing and reporting mechanisms allow organizations to efficiently monitor, report, and adjust their security posture in real time, thus ensuring ongoing regulatory adherence across dynamic and complex hybrid infrastructures (Srinivas et al., 2019). Designing a unified security framework for hybrid cloud and on-premise integrations is essential for ensuring data protection, operational efficiency, and regulatory compliance. Key components such as secure access control and identity management, integrated security monitoring and incident detection, security automation and orchestration, and compliance and regulatory considerations provide a comprehensive approach to securing hybrid environments. As organizations continue to expand their hybrid cloud infrastructures, the development and implementation of such a framework will become a fundamental step in protecting sensitive data and ensuring the resilience of business operations.

2.3. Security Technologies for Hybrid Cloud Environments

In the context of hybrid cloud environments, where on-premise infrastructures are integrated with public and private cloud services, robust security technologies are essential to ensure the protection of sensitive data and maintain compliance. The security landscape for hybrid cloud environments is complex, requiring a mix of cloud-native security services, third-party tools, and advanced networking technologies to mitigate risks (Coyne et al., 2018). This section explores the security technologies available for securing hybrid cloud infrastructures, with a focus on cloud security tools, VPNs, SD-WAN, and multi-factor authentication.

Cloud-native security services are designed to protect cloud environments and integrate seamlessly with the cloud infrastructure, providing a layer of defense without requiring additional tools. Major cloud service providers offer a range of security solutions to address specific needs in hybrid cloud environments (Darwish et al., 2019). For example, AWS shield is a managed Distributed Denial-of-Service (DDoS) protection service that safeguards applications hosted on Amazon Web Services (AWS) against cyber-attacks. Similarly, Azure security center is a unified security management system from Microsoft that provides advanced threat protection, security posture management, and compliance monitoring across hybrid cloud and on-premise environments. These services are built to offer visibility into vulnerabilities, enable quick threat detection, and provide automated remediation. In addition to native cloud security tools, third-party security solutions are often deployed in hybrid cloud environments for additional monitoring, threat detection, and mitigation. Tools like Splunk, Palo alto networks, and Fortinet offer specialized capabilities, such as real-time security analytics, intrusion prevention, and centralized threat management across multi-cloud and on-premise environments. These third-party solutions complement cloud-native tools, offering more granular security insights and additional layers of protection, particularly in complex, multi-cloud architectures (Sharma, 2020). By integrating these tools into the hybrid environment, organizations can leverage advanced machine learning algorithms, threat intelligence, and incident response capabilities to minimize risks associated with cyber threats.

One of the foundational technologies for securing hybrid cloud environments is the Virtual private network (VPN). VPNs establish secure and encrypted communication channels between on-premise infrastructures and cloud environments, ensuring that data remains protected during transit. By extending a private network over public or shared networks, VPNs protect sensitive data from unauthorized access while maintaining secure connections between distributed hybrid environments (Ahmad et al., 2020). VPNs enable organizations to isolate their cloud resources and applications, ensuring that only authorized users and systems can interact with their cloud infrastructure, even when connected over public networks. However, as organizations scale their hybrid cloud architectures, traditional VPNs may struggle to provide the level of performance and flexibility required. This is where Software-defined wide area networks (SD-WAN) come into play. SD-WAN is a more efficient, software-driven approach to managing wide-area networks, allowing organizations to dynamically route traffic across hybrid environments. SD-WAN enhances security by incorporating encryption, traffic optimization, and automated failover, which ensures secure and reliable connections between cloud and on-premise systems. Furthermore, SD-WAN enables granular control over network traffic, allowing organizations to prioritize traffic based on business needs and security requirements. By utilizing SD-WAN, companies can efficiently manage network traffic while maintaining secure, high-performance connections between distributed systems (Alwasel et al., 2020).

To strengthen access security across hybrid cloud environments, organizations are increasingly adopting multi-factor authentication (MFA). MFA adds an extra layer of protection by requiring users to provide more than one form of identification before granting access to systems or applications (Henricks and Kettani, 2019). This could involve a combination of something the user knows (e.g., a password), something the user has (e.g., a smartphone app or

hardware token), and something the user is (e.g., biometric data like a fingerprint or facial recognition). MFA significantly reduces the risk of unauthorized access, even if one factor, such as a password, is compromised. In conjunction with MFA, granular access controls are crucial for maintaining tight security in hybrid cloud environments. By implementing role-based access control (RBAC) or attribute-based access control (ABAC), organizations can define access policies based on the roles, responsibilities, and attributes of users or devices. These policies ensure that only authorized users can access specific resources, minimizing the risk of insider threats or unauthorized data exposure. Additionally, access controls can be extended to both cloud and on-premise systems, creating a cohesive security model that spans hybrid environments. By combining MFA with granular access control mechanisms, organizations can create a robust access management system that protects against both external and internal threats (DelBene et al., 2019). Securing hybrid cloud environments requires a combination of advanced security tools, efficient networking technologies, and robust access control mechanisms. Cloud-native security solutions, such as AWS Shield and Azure Security Center, provide essential protections for cloud environments, while third-party tools enhance visibility and threat mitigation across hybrid systems. VPNs and SD-WAN offer secure, high-performance networking solutions that protect data in transit, while multi-factor authentication and granular access control ensure that only authorized users gain access to critical resources. By leveraging these technologies, organizations can enhance their security posture and effectively safeguard their hybrid cloud infrastructures from evolving cyber threats (Nina and Ethan, 2019).

2.4. Addressing Challenges and Risks

In the modern era of cloud computing, organizations increasingly rely on hybrid and multi-cloud infrastructures to enhance flexibility, scalability, and resilience. While these environments offer numerous advantages, they also present significant challenges and risks that need to be managed carefully (Shrivastava, 2018). Key issues include the complexity of managing diverse security controls, data privacy and sovereignty concerns, and the balancing act between security measures and operational efficiency.

One of the most pressing challenges organizations face in multi-cloud and hybrid cloud environments is the complexity of managing diverse security controls across multiple cloud providers and on-premise systems. Each cloud provider often has its own set of security protocols, tools, and configurations, which may not always be compatible with one another. This lack of standardization can lead to fragmentation in security management and increase the likelihood of vulnerabilities. Additionally, the integration of on-premise systems with cloud platforms further complicates security, as organizations must ensure that data and applications are securely connected across disparate environments (Hussein, 2020). Effective management of security in such diverse setups requires the implementation of a unified security strategy. Organizations must employ centralized monitoring and automated tools to manage security across different cloud providers. This can include adopting a zero-trust architecture, where every user and device is continuously authenticated and monitored regardless of its location in the network. Furthermore, advanced tools for configuration management and vulnerability scanning are critical to identify and mitigate risks associated with complex hybrid systems.

Data privacy and sovereignty are significant concerns in hybrid environments, especially as organizations navigate the complexities of data location and jurisdiction (Esposito et al., 2018). The geographic distribution of cloud services means that data can be stored in different regions, each with its own legal and regulatory framework. This creates potential risks related to compliance with local laws and international data protection regulations, such as the European Union's General Data Protection Regulation (GDPR). For example, data stored in a region with less stringent privacy laws could be vulnerable to unauthorized access or misuse. Navigating these challenges requires a thorough understanding of both the legal implications of data storage and the technical tools available to mitigate risks. Organizations must ensure that data storage locations are selected based on their compliance needs and that proper mechanisms, such as encryption and anonymization, are in place to protect sensitive information. Additionally, cloud providers must offer transparency in terms of where data is stored and how it is handled across borders. Hybrid cloud models, in particular, need robust data governance frameworks to ensure that data remains compliant with relevant laws while facilitating seamless operations across environments (Celesti et al., 2019).

Another critical issue in hybrid cloud environments is ensuring that robust security measures do not hinder the performance or scalability of the infrastructure. Security measures, such as encryption, access controls, and real-time monitoring, are essential to protect data and systems from cyber threats (Asghar et al., 2019). However, if these measures are not implemented efficiently, they can introduce latency, reduce system performance, or complicate the scalability of cloud applications. To balance security with operational efficiency, organizations must adopt a risk-based approach, evaluating the security needs of each component of their hybrid infrastructure and applying security measures accordingly. For instance, critical systems and sensitive data may require high levels of encryption and multi-factor authentication, while less sensitive workloads might have less stringent security protocols. Additionally,

organizations can leverage technologies such as cloud-native security tools, which are specifically designed to scale with cloud environments without compromising performance (Laszewski et al., 2018). Automation also plays a crucial role in streamlining security operations, allowing for real-time threat detection and rapid response without placing a significant burden on system resources. The challenges and risks associated with hybrid and multi-cloud environments require a nuanced approach that considers both technical and regulatory aspects. Managing the complexity of security controls, addressing data privacy and sovereignty concerns, and balancing security with operational efficiency are key to ensuring the safe and effective use of cloud infrastructures. By adopting comprehensive strategies, leveraging advanced tools, and ensuring compliance with relevant regulations, organizations can successfully navigate these challenges and harness the full potential of hybrid and multi-cloud environments (Sivakumar and Kumar, 2019; Godbole, 2019).

2.5. Future Trends in Hybrid Cloud Security

As organizations continue to embrace hybrid cloud environments for their flexibility and scalability, ensuring robust security remains a significant challenge. The dynamic and multifaceted nature of hybrid cloud systems introduces unique security risks that require innovative solutions (Gudimetla and Kotha, 2019). In the coming years, hybrid cloud security will be shaped by emerging technologies such as artificial intelligence (AI), machine learning (ML), quantum computing, and the evolution of cloud security frameworks. These advancements will provide new ways to predict, prevent, and mitigate threats while ensuring compliance with evolving standards.

Artificial intelligence (AI) and machine learning (ML) are poised to play a transformative role in the future of hybrid cloud security (Gill et al., 2019). AI and ML technologies offer the potential to predict and prevent security threats with unprecedented accuracy. By analyzing vast amounts of data and identifying patterns, AI and ML can detect anomalies that might otherwise go unnoticed by traditional security tools. This proactive threat detection is essential in hybrid cloud environments where data is spread across multiple platforms and security breaches can occur quickly. Moreover, AI and ML can enhance automated threat detection and response capabilities. Once a security threat is identified, these technologies can initiate real-time responses, such as isolating affected systems, blocking malicious traffic, or alerting security teams for further investigation. This automation can reduce response times, minimize human error, and improve the overall efficiency of security operations. Additionally, AI and ML algorithms can continuously evolve by learning from new data, enhancing their ability to detect sophisticated threats, such as advanced persistent threats (APTs) and zero-day exploits (Parrend et al., 2018).

As hybrid cloud environments grow more complex, the need for integrated and adaptive security frameworks becomes critical. Future advancements in cloud security frameworks will focus on providing seamless integration across multi-cloud and on-premise systems, ensuring that security controls are consistent and effective across diverse environments. These frameworks will evolve to address new risks and incorporate emerging technologies, offering more dynamic and flexible security models that can scale with the organization's needs. One significant trend in the evolution of cloud security frameworks is the growing importance of compliance. As regulatory environments become more stringent, organizations will need frameworks that not only address technical security but also align with evolving compliance standards. Cloud service providers are likely to integrate compliance capabilities directly into their security frameworks, offering tools to help organizations meet the requirements of various data protection regulations, such as the GDPR, the California Consumer Privacy Act (CCPA), and other global data sovereignty laws (Ali et al., 2020). This integration will help simplify compliance management, ensuring that organizations can maintain security and privacy while meeting legal obligations in a multi-cloud environment.

Quantum computing represents one of the most transformative technologies in the future of cloud security, with the potential to significantly impact encryption and security protocols. Quantum computers can process vast amounts of data at speeds that far exceed traditional computers, which raises concerns about the security of current encryption methods. Many of the cryptographic techniques used today, such as RSA and ECC (Elliptic Curve Cryptography), rely on the difficulty of factoring large numbers or solving complex mathematical problems. However, quantum computers have the potential to break these encryption algorithms with ease, rendering existing security protocols vulnerable. As quantum computing advances, hybrid cloud security will need to evolve to incorporate quantum-resistant cryptographic algorithms. Researchers are already developing post-quantum cryptography (PQC) algorithms that are designed to withstand the power of quantum computers. These algorithms will play a crucial role in safeguarding sensitive data stored and processed in hybrid cloud environments. Additionally, cloud service providers will need to implement quantum-safe security protocols to ensure that their infrastructures remain secure in the quantum era. This transition to quantum-resilient encryption will be a significant challenge, requiring a coordinated effort between cloud providers, researchers, and industry stakeholders to ensure the continued security of hybrid cloud systems. The future of hybrid cloud security will be shaped by the integration of cutting-edge technologies such as AI, ML, and quantum

computing, as well as the evolution of cloud security frameworks. AI and ML will enhance threat detection and response capabilities, making hybrid cloud environments more secure and efficient (Chirra, 2020). As cloud security frameworks evolve, they will better address the complexities of multi-cloud environments and ensure compliance with increasingly stringent regulations. Finally, quantum computing will present both challenges and opportunities for cloud security, particularly in the area of encryption, necessitating the development of quantum-resistant security protocols. Together, these advancements will drive the next generation of hybrid cloud security, providing organizations with the tools they need to protect their data and infrastructure in a rapidly changing technological landscape.

3. Conclusion

The unified security framework presented in this review aims to address the complex challenges associated with securing hybrid cloud and on-premise integrations. This framework integrates advanced technologies such as artificial intelligence (AI), machine learning (ML), and post-quantum cryptography to enhance threat detection, response, and data protection. By unifying security controls across disparate cloud providers and on-premise systems, the framework ensures consistent and scalable protection while maintaining compliance with evolving regulations. Key components of the framework include automated threat detection, AI-driven security monitoring, adaptive security policies, and robust encryption protocols. The framework's role is pivotal in offering a comprehensive, proactive approach to securing hybrid infrastructures, ensuring both resilience and efficiency in managing security risks.

For organizations seeking to implement the proposed security model, several strategic recommendations should be considered. First, organizations should prioritize the adoption of AI and ML technologies for real-time threat detection and automated response, enabling faster identification and mitigation of security risks. Additionally, cloud and on-premise integration should be carefully planned to ensure that security controls are seamlessly applied across all environments, minimizing vulnerabilities due to fragmentation. Organizations must also stay ahead of regulatory changes by adopting frameworks that integrate compliance tools, ensuring continuous alignment with data protection laws and industry standards. Furthermore, as quantum computing poses future threats to encryption, organizations should invest in researching and transitioning to post-quantum cryptography solutions, ensuring that their security protocols remain resilient to emerging threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abualkishik, A.Z., Alwan, A.A. and Gulzar, Y., 2020. Disaster recovery in cloud computing systems: An overview. *International Journal of Advanced Computer Science and Applications*, *11*(9).

[2] Ahmad, S., Mehfuz, S. and Beg, J., 2020, December. Securely work from home with CASB policies under COVID-19 pandemic: a short review. In *2020 9th International conference system modeling and advancement in research trends (SMART)* (pp. 109-114). IEEE.

[3] Ali, O., Shrestha, A., Chatfield, A. and Murray, P., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), p.101419.

[4] Alwasel, K., Jha, D.N., Hernandez, E., Puthal, D., Barika, M., Varghese, B., Garg, S.K., James, P., Zomaya, A., Morgan, G. and Ranjan, R., 2020. Iotsim-sdwan: A simulation framework for interconnecting distributed datacenters over software-defined wide area network (sd-wan). *Journal of Parallel and Distributed Computing*, *143*, pp.17-35.

[5] Anand, D. and Khemchandani, V., 2019. Identity and access management systems. *Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions*, p.61.

[6] Anisetti, M., Ardagna, C., Cremonini, M., Damiani, E., Sessa, J. and Costa, L., 2020. Security threat landscape. *White Paper Security Threats*.

[7] Asghar, M.R., Hu, Q. and Zeadally, S., 2019. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, p.106946.

[8] Cai, C., Mei, S. and Zhong, W., 2019. Configuration of intrusion prevention systems based on a legal user: the case for using intrusion prevention systems instead of intrusion detection systems. *Information Technology and Management*, *20*, pp.55-71.

[9] Celesti, A., Fazio, M., Galletta, A., Carnevale, L., Wan, J. and Villari, M., 2019. An approach for the secure management of hybrid cloud–edge environments. *Future Generation Computer Systems*, *90*, pp.1-19.

[10] Chiranjeevi, H.S., Shenoy, M.K. and Sundar, D.S., 2018. Integrating on-premises data with customer relationship management application on cloud: A hybrid IT infrastructure support service. *Cogent Engineering*, *5*(1), p.1462755.

[11] Chirra, D.R., 2020. AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. *Revista de Inteligencia Artificial en Medicina*, *11*(1), pp.382-402.

[12] Coyne, L., Dain, J., Forestier, E., Guaitani, P., Haas, R., Maestas, C.D., Maille, A., Pearson, T., Sherman, B. and Vollmar, C., 2018. *IBM private, public, and hybrid cloud storage solutions*. IBM Redbooks.

[13] Darwish, A., Hassanien, A.E., Elhoseny, M., Sangaiah, A.K. and Muhammad, K., 2019. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. *Journal of Ambient Intelligence and Humanized Computing*, *10*, pp.4151-4166.

[14] DelBene, K., Medin, M. and Murray, R., 2019. The Road to Zero Trust (Security). *DIB Zero Trust White Paper*, *9*.

[15] Duncan, B. and Zhao, Y., 2018, July. Risk management for cloud compliance with the EU General Data Protection Regulation. In *2018 International Conference on High Performance Computing & Simulation (HPCS)* (pp. 664-671). IEEE.

[16] El Sibai, R., Gemayel, N., Bou Abdo, J. and Demerjian, J., 2020. A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, *31*(2), p.e3720.

[17] Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y. and Choo, K.K.R., 2018. On data sovereignty in cloud-based computation offloading for smart cities applications. *IEEE Internet of Things Journal*, *6*(3), pp.4521-4535.

[18] Gade, K.R., 2020. Data Mesh Architecture: A Scalable and Resilient Approach to Data Management. *Innovative Computer Sciences Journal*, *6*(1).

[19] Gill, S.S., Tuli, S., Xu, M., Singh, I., Singh, K.V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U. and Pervaiz, H., 2019. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things*, *8*, p.100118.

[20] Godbole, M.V., 2019. Compliance Challenges and Solutions: Ensuring Regulatory Adherence in ERP Systems for Finance in Banking. *International Meridian Journal*, *1*(1), pp.1-10.

[21] Gudimetla, S.R. and Kotha, N.R., 2019. The Hybrid Role: Exploring The Intersection Of Cloud Engineering And Security Practices. *Webology (ISSN: 1735-188X)*, *16*(1).

[22] Gundu, S.R., Panem, C.A. and Thimmapuram, A., 2020. Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing. *SN Computer Science*, *1*(5), p.256.

[23] Hale, M.L. and Gamble, R.F., 2019. Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information security control standards. *Requirements Engineering*, *24*, pp.365-402.

[24] Hartzog, W. and Richards, N., 2020. Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, p.1687.

[25] Henricks, A. and Kettani, H., 2019, October. On data protection using multi-factor authentication. In *Proceedings of the 2019 International Conference on Information System and System Management* (pp. 1-4).

[26] Hiran, K.K., Doshi, R., Fagbola, T. and Mahrishi, M., 2019. *Cloud computing: master the concepts, architecture and applications with real-world examples and case studies*. Bpb Publications.

[27] Hussein, A.A., 2020. Data migration need, strategy, challenges, methodology, categories, risks, uses with cloud computing, and improvements in its using with cloud using suggested proposed model (DMig 1). *Journal of Information Security*, *12*(1), pp.79-103.

[28] Indu, I., Anand, P.R. and Bhaskar, V., 2018. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, *21*(4), pp.574-588.

[29] Kamal, M.A., Raza, H.W., Alam, M.M. and Mohd, M., 2020. Highlight the features of AWS, GCP and Microsoft Azure that have an impact when choosing a cloud service provider. *Int. J. Recent Technol. Eng*, *8*(5), pp.4124-4232.

[30] Kumar, R. and Goyal, R., 2020. Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). *Computers & Security*, *97*, p.101967.

[31] Kure, H.I., Islam, S. and Razzaque, M.A., 2018. An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), p.898.

[32] Laszewski, T., Arora, K., Farr, E. and Zonooz, P., 2018. *Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud*. Packt Publishing Ltd.

[33] Megouache, L., Zitouni, A. and Djoudi, M., 2020. Ensuring user authentication and data integrity in multi-cloud environment. *Human-centric Computing and information sciences*, *10*, pp.1-20.

[34] Mthunzi, S.N., Benkhelifa, E., Bosakowski, T., Guegan, C.G. and Barhamgi, M., 2020. Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems*, *107*, pp.620-644.

[35] Mughal, A.A., 2019. Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. *Applied Research in Artificial Intelligence and Cloud Computing*, *2*(1), pp.1-31.

[36] Muhammad, T., 2019. Revolutionizing Network Control: Exploring the Landscape of Software-Defined Networking (SDN). *International Journal of Computer Science and Technology*, *3*(1), pp.36-68.

[37] Muhammad, T., Munir, M.T., Munir, M.Z. and Zafar, M.W., 2018. Elevating Business Operations: The Transformative Power of Cloud Computing. *International Journal of Computer Science and Technology*, *2*(1), pp.1-21.

[38] Nina, P. and Ethan, K., 2019. AI-Driven Threat Detection: Enhancing Cloud Security with Cutting-Edge Technologies. *International Journal of Trend in Scientific Research and Development*, *4*(1), pp.1362-1374.

[39] Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A. and Brown, J., 2020. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, *9*(2), p.44.

[40] Okechukwu, N.D., Osuagwu, O.E. and Ekwonwune, E.E., 2018. A Hybrid Implementation of Encryption and Decryption Algorithms for Data Security in Cloud Computing. *West African Journal of Industrial & Academic Research*, *19*(2), p.70.

[41] Parrend, P., Navarro, J., Guigou, F., Deruyver, A. and Collet, P., 2018. Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. *EURASIP Journal on Information Security*, *2018*, pp.1-21.

[42] Plá, L.F., Shashidhar, N. and Varol, C., 2020, June. On-premises versus SECaaS security models. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.

[43] Pookandy, J., 2020. End-to-end encryption and data integrity verification in cloud CRM as a framework for securing customer communications and transactional data. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), pp.19-32.

[44] Raj, P., Raman, A., Raj, P. and Raman, A., 2018. Multi-cloud management: Technologies, tools, and techniques. *Software-Defined Cloud Centers: Operational and Management Technologies and Tools*, pp.219-240.

[45] Ranise, S., Sciarretta, G. and Tomasi, A., 2019, November. Enroll, and Authentication Will Follow: eID-Based Enrollment for a Customized, Secure, and Frictionless Authentication Experience. In *International Symposium on Foundations and Practice of Security* (pp. 156-171). Cham: Springer International Publishing.

[46] Sehgal, N.K., Bhatt, P.C.P. and Acken, J.M., 2020. *Cloud computing with security and scalability*. Springer, https://link. springer. com/book/10.1007/978-3-031-07242-0.

[47] Sharma, H., 2020. Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on interoperability and comprehensive visibility. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), pp.1-18.

[48] Sharma, H., 2020. Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on

interoperability and comprehensive visibility. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), pp.1-18.

[49] Shneiderman, B., 2020. Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *10*(4), pp.1-31.

[50] Shrivastava, P., 2018. Environmental technologies and competitive advantage. In *Business Ethics and Strategy, Volumes I and II* (pp. 317-334). Routledge.

[51] Sivakumar, R. and Kumar, L., 2019. Unlocking Organizational Potential: The Synergy of Performance Management and Knowledge Management. *Journal of Business and Economic Options*, *2*(4), pp.159-165.

[52] Spirin, O., Oleksiuk, V., Balyk, N., Lytvynova, S.H. and Sydorenko, S., 2019. The blended methodology of learning computer networks: Cloud-based approach. In *Proceedings of the 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer* (Vol. 2, No. 2393, pp. 68-80). CEUR Workshop Proceedings.

[53] Srinivas, J., Das, A.K. and Kumar, N., 2019. Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, pp.178-188.

[54] Sunyaev, A. and Sunyaev, A., 2020. Cloud computing. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, pp.195-236.

[55] Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.

[56] Tan, C.B., Hijazi, M.H.A., Lim, Y. and Gani, A., 2018. A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends. *Journal of Network and Computer Applications*, *110*, pp.75-86.

[57] Tchernykh, A., Schwiegelsohn, U., Talbi, E.G. and Babenko, M., 2019. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, p.100581.

[58] Trakadas, P., Nomikos, N., Michailidis, E.T., Zahariadis, T., Facca, F.M., Breitgand, D., Rizou, S., Masip, X. and Gkonis, P., 2019. Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture. *Sensors*, *19*(16), p.3591.

[59] Yan, X. and Wang, H., 2020. Survey on zero-trust network security. In *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part I 6* (pp. 50-60). Springer Singapore.

[60] Zhou, L., Fu, A., Yu, S., Su, M. and Kuang, B., 2018. Data integrity verification of the outsourced big data in the cloud environment: A survey. *Journal of Network and Computer Applications*, *122*, pp.1-15.